Authentication and Password Management

Paul Mooney
Chief Software Architect, Microsoft MVP

@daishisystems | www.insidethecpu.com

Overview

Authentication and Password Management

- Implement secure authentication
- Communicate authentication data
- Implement secure password storage
- Implement secure password validation
- Use password encryption techniques
- Protect sensitive data

Communicating Authentication Data

Authentication

- Types of authentication
- Common authentication protocols
- Secure communication protocols
- bcrypt demo
- Hashing
- Salting

Types of Authentication

- Single-factor authentication
- Multi-factor authentication
- Biometric authentication

Single-factor authentication

- Single factor for identification
- Easy to implement
- Least secure

Multi-factor authentication

- Multiple factors of identification
- More secure than single-factor
- More complex to implement

Biometric authentication

- Physical or behavioral characteristic
- Most secure type of authentication
- Expensive and difficult to implement

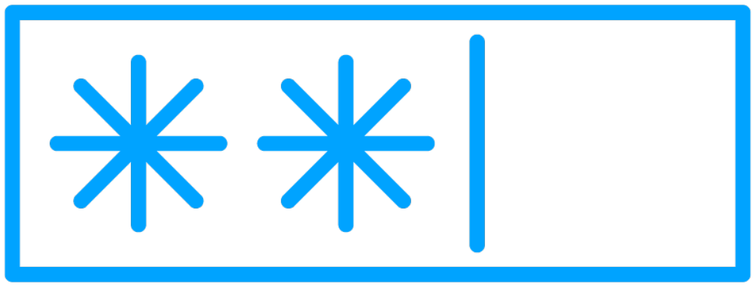
Common Authentication Protocols

- OAuth and OpenID Connect
- Limited access to resources
- 3rd party authentication
- Complex implementation
- Standardized way to authenticate users
- Use secure transport protocols
- Validate all input data
- Principle of least privilege
- Stay up to date

Secure Communication Protocols

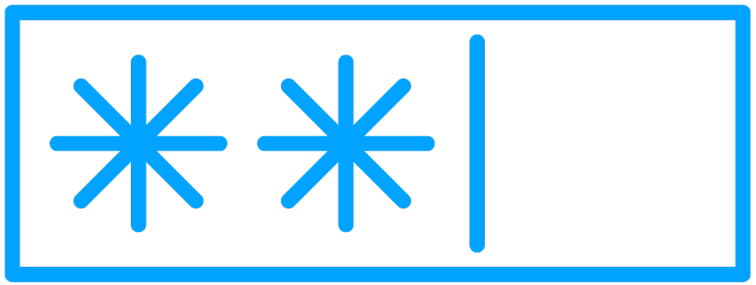
- Transport Layer Security (TLS)
- Secure Sockets Layer (SSL)
- Properly configuring certificates
- Disable outdated cryptographic ciphers
- Apply the latest security patches
- Use HTTP POST

Validating & Storing Authentication Data



Password Security Best Practices

- Hashing
- Salting
- Encryption



Password Policies

- Password length
- Password complexity
- Expiration date

Password Storage Options

Hashing

Fixed length

Encrypted

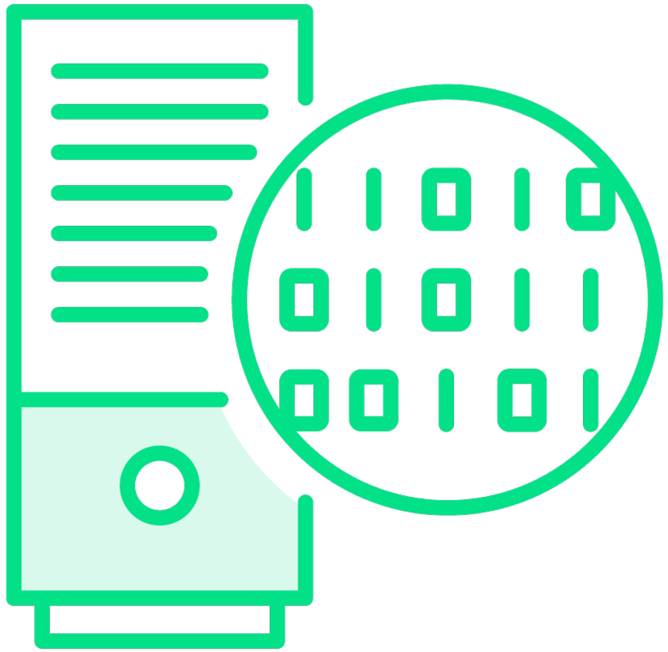
One-way

Salting

Random characters

Precomputed hash tables

Unique per password

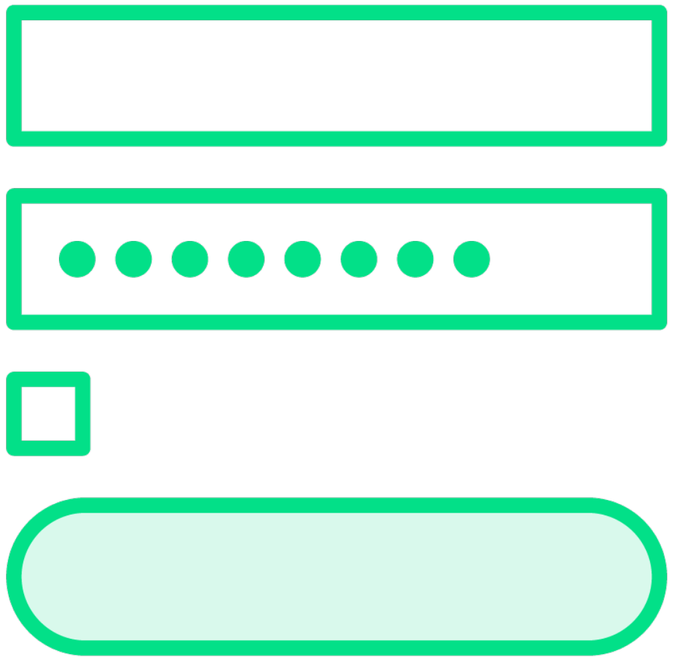


Supported Hashing Algorithms

- Bcrypt
- Scrypt
- Salt value per password

Demo

Single-factor Authentication



Password Policies

- Password complexity
- Hashing
- Salting
- Expiration
- Account lockout
- Policies versus convenience

Password Reset

- Requesting a reset
- Token storage
- Reset link generation
- Reset password page
- Password update
- Token expiration
- Token revocation
- Logging
- Error handling

Demo

Multi-factor Authentication

Summary

Authentication & Password Management

- Secure implementation guidelines
- Authentication types
- Common protocols
- Secure communication protocols
- Password security best practices
- SFA and MFA demos